Empirical Study for Performance Analysis of IPv6 Networks and Tunnel Broker Mechanism

Yousaf Saeed[1], Dr. Khalil Ahmed[2], Dr. Mahi Lohi[3], Sagheer Abbas[4], Atifa Athar[5]

[1]Department of Computer Science, NCBA&E Lahore, Punjab, Pakistan
[2]Department of Computer Science, NCBA&E Lahore, Punjab, Pakistan
[3]Department of Engineering, University of Westminster, London, UK
[4]Department of Computer Science, NCBA&E Lahore, Punjab, Pakistan
[5]Department of Computer Science, NCBA&E Lahore, Punjab, Pakistan

***Abstract* - In today's technological developments, aside from hardware and software expansions, data communication is equally important. The role of internet protocol address plays a vital role in data communication and with the depletion rate of IPv4 addresses, it is highly essential to adopt IPv6 as this is going to be the next protocol addresses of communication devices. This paper shows research on a number of transition methods for IPv6 where experiments are carried out at two different levels. IPv6 network has been established successfully in computer lab followed by residential setup. Performance of IPv6 is found by comparing it with the current IPv4 setup, and aspects including congestion and speed are taken into account as performance measures. Practical work on Tunnel Broker transition mechanism is performed and WireShark simulator has been used to carry out performance analysis of IPv4 and IPv6 and the results are achieved specifying that IPv6 functions better than IPv4 in the proposed network setup.**

Keywords *– IPv6; IPv4; DHCPv6; DNS; Tunnel Broker*

I. INTRODUCTION

Internet Engineering Task Force (IETF) proposed IPv6 in order to provide large address space to IPs [1]. Work on protocol design has been done already in the past years along with the transition mechanisms [2][3] of IPv6, however, still it is required to be studied further for performance analysis. Protocol transitions are essential to be carried out these days due to shortage of IPv4 addresses. These protocol transitions are challenging and not easy especially considering the transition from IPv4 to IPv6. Protocol transition requires the installation and configuration of this new protocol (IPv6) on all the nodes within a network and to ensure its successful functionality. This might be a bit simple in case of small network but challenging in large networks as this shift requires implementation of infrastructure that should support IPv6 and the configuration involved. Transition phase is not simple and will take years for full functional IPv6 deployment in the world. It is in fact a step by step process while reaching the case of full functional independent IPv6 deployment. Therefore, being a step by step process, equal considerations must be given to both IPv4 and IPv6 as this shift cannot be achieved in an abrupt manner. It is important to highlight the importance of nodes as they provide means for communication and in IPv4 and IPv6 environment, such nodes are categorized as IPv4-only, IPv6-only, IPv4, IPv6 and IPv6 over IPv4. It is important to metion that selecting tunnel broker is due to the fact that not every router fully supports IPv6.

Section II of this paper provides different transition mechanisms necessary for IPv6 deployment. Section III highlights the existing problems with these transition mechanisms that need considerations. In Section IV and V, practical work is carried out in computer lab and residential environment respectively in order to find the performance measures of IPv4 and IPv6 using WireShark simulator.

II. TRANSITION MECHANISMS

A number of transition mechanisms are used to deploy IPv6 that include its compatibility with IPv4 as highlighted below:

A. Dual Stack

Dual stack consist of both the stacks of IPv4 and IPv6 protocols. In such system, we have both the protocols working with certain techniques to make the communication possible. In dual stack, we have IPv4 to IPv6 communication scheme in which IPv4

communication is made possible over an IPv6-only network.

A node can be configured to support both the protocols of IPv4 and IPv6, however, one of the stacks might be disabled for operational purposes. A node (IPv4/IPv6 enabled) having its IPv4 stack disabled will operate like IPv6-only node and the node having its IPv6 stack disabled will work like IPv4-only node and defined in [4]. Also, the configured tunnel technique may and may not be used in addition to dual stack operation. It depends on the situation how communication between nodes can take place. Figure 1.1 elaborates dual stack system in terms of IPv4 and IPv6.

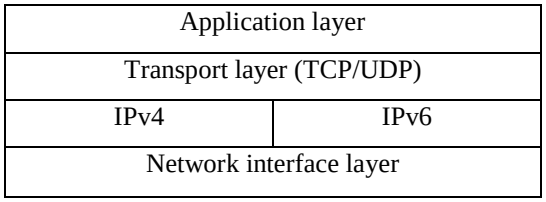

Figure 1.1: Dual stack systems [5]

B. Tunneling

Tunneling is a virtual point to point connection and provides a means of utilizing the existing IPv4 infrastructure to carry IPv6 traffic. One tunnel provides one channel for the encapsulated packets to transfer. Encapsulation and decapsulation of packets is done at both ends of a tunnel. Here tunneling refers to the whole process from data encapsulation, data transfer and data decapsulation. IPv4/IPv6 nodes can tunnel IPv6 datagrams by encapsulating them in IPv4 packets and sends them over IPv4 networks.
An IPv4/IPv6 node creates a tunnel by encapsulating IPv4 header and transmits the encapsulated packet. At the receiver side, IPv4/IPv6 node receives the encapsulated packet, decapsulates it, remove the IPv4 header and process the IPv6 packet [6] as shown in Figure 1.2.

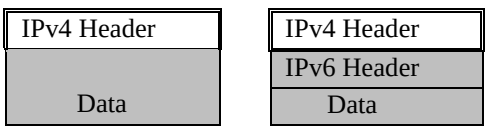

Figure 1.2: IPv6 packet encapsulated by IPv4 [6]

C. Translation

Translation is the process of translating an IPv6-only host to access IPv4-only internet resources or to translate IPv4-only host to access IPv6-only network resources.

Translation mechanism is different from tunneling in that it made communication possible between the nodes that use a single protocol system like one system might be IPv4-only node while other system might be IPv6-only node. So the communication between nodes having single protocol is done successfully by translation mechanism and defined in [7]. NAT-PT uses IP translation that is called Stateless IP/ICMP Translation (SIIT). SIIT is a mechanism which translates an IPv6 host to IPv4 host and vice versa.

III. PROBLEMS WITH EXISTING TRANSITION MECHANISMS

All of these transitions methods face certain problems despite of the fact that they are facilitating the way for future internet. In dual stack, security must be kept under consideration for IPv6 networks as we do not have the required system for it. There are a number of IPv6 vendors now who are making the required hardware having the facilities for IPv6 but still more need to be done such as configuration, IPv4 address requirements and administrative overhead.

Although IPv6 tunneling is widely available, however, the associated limitation is it requires a thorough understanding of internet technologies and appropriate software to be installed. This makes it most suitable for organizations having system administrators. We have manual tunneling and automatic tunneling mechanisms and the limitation of tunneling applies to them as well.
Tunnel brokers [8], where they facilitate users nowadays have a number of issues elaborates as follows:

i) Tunnel broker is a manual configuring tunneling mechanism and needs manual configuration to set up. It has the issue that the host behind a NAT box cannot use the services of the tunnel broker to access IPv6 contents. It uses routable IPv4 address and does not work with private addresses; therefore, communication with IPv6 systems in a network to use services can only take place if you are not behind a NAT router.

ii) It needs configuration to be in the client system before communicating through the tunnel.

iii) Tunnel broker transition mechanism has the limitation of being a single point of failure. If the tunnel broker gets down, clients cannot get any tunnels for communication with IPv6 networks.

iv) When the number of clients increases, the number of tunnels also increases and currently tunnel broker is not able to handle huge amount of tunnels to be configured and as a result it acts as a bottleneck.

v) Security problems also exists as when IPv4 and IPv6 server address is configured by the tunnel broker and sent along with the configuration parameters then it is possible for anyone to scan the packets with the packet scanner that supports IPv6 packets and as a result middle man can know exactly what has been sent.

vi) When the tunnels are created, the active tunnels consume more processing power and tunneling resources, hence processing overhead and tunnel complexity results.

These are some issues in tunnel broker mechanisms that need to be addressed. Our practical work is focused on the same tunnel broker concept in order to address these issues from communications perspective i.e. to find whether IPv4 or IPv6 packets are suitable for it and under what circumstances.

IV. LAB SCENARIO

Practical work of transition mechanism is carried out in the computer laboratory at Westminster University where a network of IPv6 systems is created. For functionality of IPv6 network, a manual tunnel broker mechanism was selected. Five computer systems having Microsoft Windows 7 operating systems were selected for practical work and scanned by anti-virus software to remove performance doubts during the experiment. Ethernet switch (3com) was used to connect all these computers systems together. Figure 1.3 indicates our established network of five computer systems and their linkages with the attached Ethernet switch (3com).

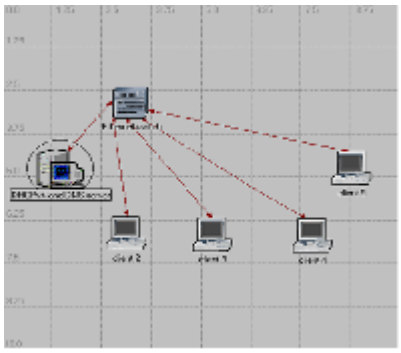

Figure 1.3: Infrastructure of the established network

One computer system on the network was selected as a server by installing *Dibbler 0.7.2 (server part)* which is an open source software and has support for windows operating system for providing Dynamic Host Configuration Protocol (DHCP) for IPv6 based computers on a network. Domain Name System (DNS) for IPv6 is also configured using *Dibbler 0.7.2* and after a number of unsuccessful attempts, finally succeeded to assign DNS names for the number of client systems used in the network. Rest of the clients were installed with clients parts of Dibber 0.7.2 in order to automatically receive DHCP and DNS packets from the server upon initializing.

This resulted in a full functional IPv6 network where every node was communicating perfectly with one another. Stateful address configuration in the form of DHCPv6 was working perfectly; automatic addresses were seamlessly assigned by the DHCPv6 server from the pool of addresses to the clients and DNS was configured for the systems as well. Hence, we have IPv6 network communicating with each other and given DHCPv6 and DNS services to the clients in the established network. After running configuration files in DHCPv6 server and the clients, packet sniffer application called *wireshark* was initialized in server and in all the client systems in order to capture IPv6 packets from the server. IPv6 and IPv4 filters were applied both in server and client systems and results were obtained as shown in Figure 1.5 and 1.4 respectively.

In Figure 1.4, IPv6 and IPv4 packets filtering is performed. The red line shows IPv6 protocols and the blue line indicates IPv4 protocols. As both color of lines are steady at certain length of time till 20 seconds, this indicates that server received the

request from clients for IP addresses after 20 seconds. Afterwards, it can be seen that IPv4 packets were received first followed by IPv6 packets. Also if we see the amount of generated packets here, significantly less number of IPv6 packets are identified then IPv4 packets, thereby producing comparatively less congestion.

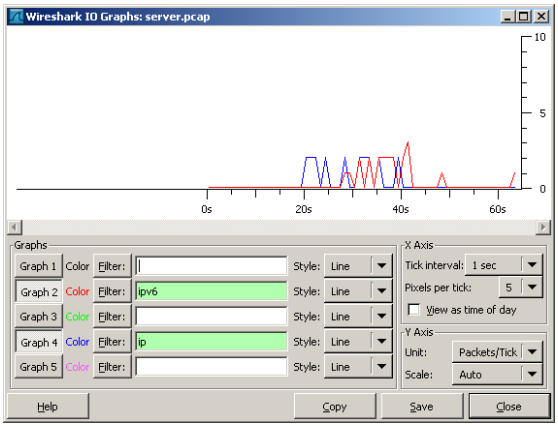

Figure 1.4: Filtered IPv6 and IPv4 packets in DHCPv6 server

Now considering Figure 1.5, the red and black lines indicates IPv6 and IPv4 packets respectively. Here, the client is waiting to receive IP addresses to be assigned by the server and nearly around 20 seconds, the client started receiving IP addresses. Upon filtering, we find that IPv4 packets were received first followed by IPv6 packets. Also, if we see the amount of generated packets, again considerably less number of IPv6 packets are used as compared to IPv4 packets.

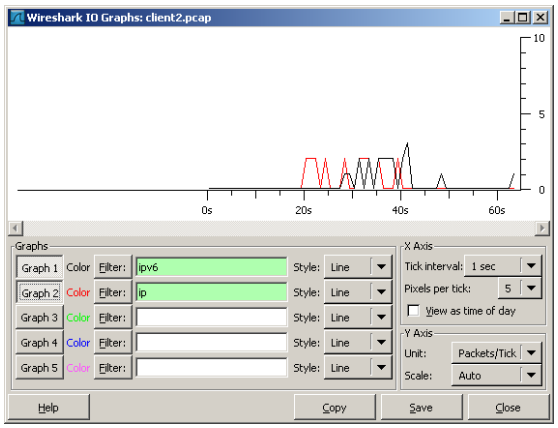

Figure 1.5: Filtered IPv6 and IPv4 protocol comparison in DHCPv6 client

V. RESIDENTIAL SCENARIO

At the residential part, tunnel broker is selected in order to use its services online. The reason is that it is similar to a virtual IPv6 Internet Service Provider that provides IPv6 communication services to clients and that can be a good option for experimentation by a third person service provider.

A. Tunnel Broker Setup

After a number of unsuccessful attempts tunnel broker setup was created as indicated in Figure 1.6 and the tunnel service was obtained from the tunnel broker and was availed by searching a number of tunnel brokers online who offer their services for the creation of a tunnel and allow users to take advantage of the new technology. Tunnel broker services were taken first by selecting a tunnel setup provider *hurricane electric internet services*. By visiting their website which had a requirement of registration and giving them the details which are needed for security purposes like prevention of unauthorized access to the tunnels. All such details were provided to the tunnel broker. The user identity name during registration process is kept in their DNS system. Upon acceptance, our IPv4 address was given to hurricane electric which was required for tunnel setup purpose. Of the list of tunnel servers, a tunnel server in *Los Angeles, United States* was selected. The selection of such a place was because of the long distance of the tunnel server as shown in Figure 1.7. The motive was actually to select long distance for performance evaluation.

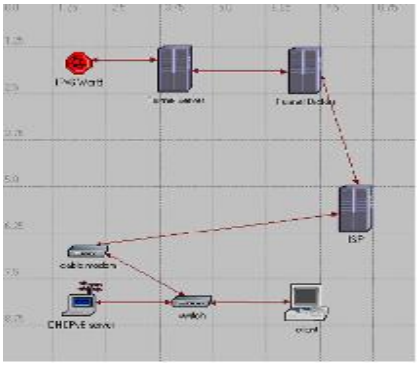

Figure 1.6: Interaction of tunnel setup by Tunnel Broker

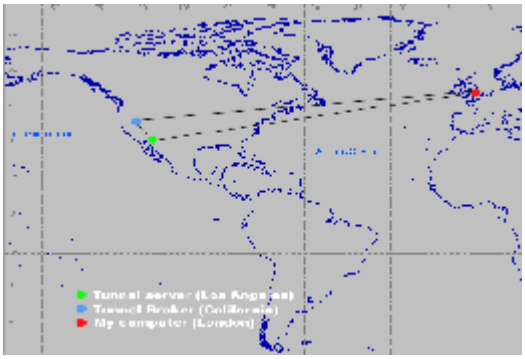

Figure 1.7: Distance of tunnel server and the client

Our computer system having Windows Operating System communicated with the tunnel broker and has been provided with tunnel setup parameters by configuring the system and as a result IPv6 services were allowed which were in the form of allowing IPv6 based websites. As this is a transition phase, therefore, IPv6 website administrators have included certain mechanisms that shows proof of successful IPv6 connectivity and to use its services of IPv6 by the clients.

Project *KAME* [9] highlights certain animation on its site for confirmation that IPv6 connectivity and its services are availed successfully, which on the other hand cannot be seen with IPv4 address connectivity with the tunnel broker. The animation was seen successfully with IPv6 address connectivity.

By visiting www.kame.net on IPv6 based connectivity, wireshark was used in order to capture IP packets. Upon applying filters, results were obtained as indicated in Figure 1.8 that shows the tunnel setup time at the tunnel broker. It shows red line representing IPv4 packets and blue line representing IPv6 packets. When filtered with IPv4 and IPv6 protocols, it was found that after 5 seconds, high number of IPv4 packets were traced than IPv6 packets. This shows the infancy of initial phases of IPv6 deployment by the tunnel broker. Again less number of IPv6 packets were seen as compared to IPv4 packets.

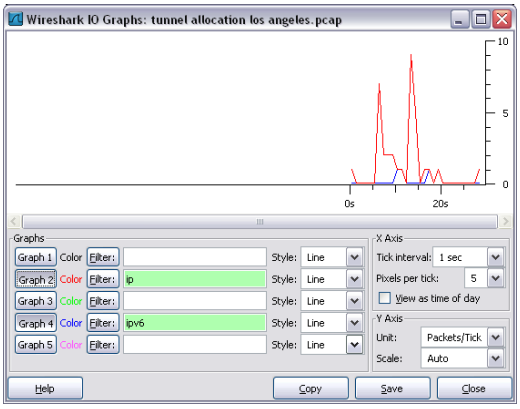

Figure 1.8: IPv6 and IPv4 tunnel setup time

VI. CONCLUSION

It is concluded that tunnel broker is the existing transition scheme that is going to take users to the next level of internet technology as it acts like a virtual Internet Service Provider of IPv6 that offers IPv6 services to its clients. Results gained from the experiments carried out in different environments shows that in server machine, comparatively less number of IPv6 packets are utilized in a DHCPv6 environment to assign automatic IPv6 address to the clients as compared to IPv4, thus creating less congestion. However, when we talk about quick response time or speed of IPv6 protocol in a server machine, it is found that IPv6 protocol is not quick enough to respond in a DHCPv6 environment, thus it is slower than IPv4.

Moreover, when IPv6 protocol is used in DCHPv6 clients to receive automatic IPv6 addresses from the server machine, it is found that IPv6 is slower to respond than IPv4; and during this approach less amount IPv6 packets were found, thus again creating less congestion. Another important conclusion is the amount of time that a tunnel broker takes in configuring the tunnel for a client end point and sending the relevant configuration parameters to the user collectively. It has been found that during this phase, less number of IPv6 packets are used as compared to IPv4 thus generating less congestion, however, speed wise IPv4 was quick to respond than IPv6.

VII. FUTURE WORK

There are multidisciplinary areas where IPv6 can be deployed based on its associated performance aspects. IPv6 in vehicular communication can better utilize its frequency allotment, nodal communication, and providing security. Other areas for its utilization are connectivity of a node with possible communication devices like internet of things. Moreover, because of its large pool of addresses, Artificial Intelligence based devices can be connected using IPv6.

VIII. REFERENCES

[1] A.M.S. Bradner, "IP: Next Generation (IPng), "White Paper Solicitation RFC 1550, Dec. 1993.

[2] R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, Aug. 2000

[3] I. Raicu, S. Zeadally, "Evaluating IPv4 to IPv6 Transition Mechanisms", IEEE International Conference on Telecommunications 2003, ICT 2003, Feb, 2003.

[4] E. Nordmard, R. Gilligan. (October 2005). *RFC 4213: Basic Tranition Mechanisms for IPv6 Hosts And Routers.* Available: http://www.faqs.org/rfcs/rfc4213.html. Last accessed July 2008.

[5] Joe Davies (18-4-2006). *IPv6 Transition Technologies.* Available: http://technet.microsoft.com/en-us/library/bb727021.aspx.

[6] J. Bound, L. Toutain, O. Medina, F. Dupont, H. Affi, A. Durand. (July 2002). *Dual Stack Transition Mechanism.* Available: http://www.ietf.org/proceedings/54/slides/ngtrans-7.pdf.

[7] G. Tsirtsis, P. Srisuresh. (February 2000). *Network Address Translation - Protocol Translation.* Available: http://www.ietf.org/rfc/rfc2766.txt. Last Accessed June 2012.

[8] J. Bi, J. Wu, X. Leng. (January 2007). International Journal of Computer Science and Network Security. *IPv4/ IPv6 Transition Technologies and Univer6 Architecture.* 7(1), p7.

[9] Sectors, Corporate; KAME Project, 2010.